

CURRENT APPROACHES TO ASSESSING RISK IN MAINTENANCE AND INSPECTION

Barbara G. Kanki, Ph.D.
NASA Ames Research Center

Introduction

As researchers, designers, operators, and managers of complex, high-risk operations, we share an interest in human performance tools that can help us assess and manage risk. Through effective risk management, we seek to achieve the highest levels of operational and personal safety as a top priority. At the same time, however, operations must prove themselves efficient and effective in a time of dwindling resources and an unpredictable economy. In light of these conditions, we, more than ever, need reliable and valid tools to assess risk so that resources can be managed effectively and the balance of safety and performance is optimized.

I will be describing several innovative approaches to risk that have been developing over the last five or six years. But first, I would like to introduce three types of risk in order to set up a context for describing these new approaches. The three risk types are 1) design risk, 2) process risk, and 3) the risk of human error. As their names suggest, they refer to different targets and serve different purposes although I will argue that they have been mixed and merged in a variety of helpful and unhelpful ways. In spite of the fact that the different risk types often share analysis tools, their distinct objectives and limitations should provide guidance for their best use. The new initiatives I will describe cross the boundaries of these risk types as they combine to create a more robust and expanded risk description.

Design, Process, and Human Error Risks

I do not intend to describe risk methodologies in a technically detailed way, nor do I mean to suggest that any particular tool or solution is best. Rather, I would like to describe a way of thinking about risk assessment and the importance of choosing the best set of risk assessment tools to solve particular risk management issues. Generally speaking, there is no lack of valuable methods and metrics, but the way in which they have been applied to problems has sometimes confused design, process, and human error risks

Design Risk

By design risk I refer to the risks related to engineering objects (e.g., vehicles, systems, subsystems, components), whose analyses can be used to aid design decisions. For example, loss-of-vehicle risk for the Space Shuttle can be assessed and “averaged” over mission phases and described by the relative contributions of principal vehicle elements such as orbiter, space

shuttle main engines (SSME), solid rocket boosters, external tank, etc. These elements, in turn, are described by the relative contributions of their main risk drivers. For example, turbomachinery and combustion devices are risk drivers of SSME. A typical approach for assessing design risk is probabilistic risk assessment (PRA) “a multi-disciplinary complex of techniques that integrates probabilistic reliability-availability engineering and analysis with mathematical statistics, decision theory, systems engineering, conventional engineering analysis, and even cognitive psychology.”^a Other basic techniques include hazard lists and analysis, failure modes and effects analysis (FMEA), or the combination, failure modes, effects and criticality analysis (FMECA)^b. In short, many tools exist and contribute to design PRA and their results can provide guidance for future designs (e.g., shuttle upgrades) or for design changes such as the shuttle APU system and Reusable Solid Rocket Motor. However, a strictly design PRA will be limited in its relevance to ground processing and its ability to predict or explain human error in maintenance and inspection (see Table 1).

Process Risk

As its name implies, process risk targets processes rather than objects, and its analyses are intended to aid process decisions, for example, procedures, process control, maintenance and inspection requirements, etc. (also shown in Table 1). It makes use of many of the same analysis tools and techniques that design risk employs including hazards analysis, FMEA, event trees and PRA. At times the shift from design to process creates variants of tools such as the Process FMEA (PFMEA). Although there are many schools of thought on specific methods, the focus is on identifying and evaluating process steps according to their importance to risk contributors. Some process analyses intentionally strip away all but the minimum required functional steps in order to assess the Zero Base. For example, Zero Based steps are reviewed in order to evaluate the differential risk incurred as result of the elimination of assurance related process steps. Such analyses can provide decision guidance on developing the most effective maintenance controls^c. Limitations of process risk assessment depend on the degree to which it is applied in the context of design or “hardware” risk; in some process decisions, design risk may not be a factor of concern. Limitations are also imposed by the degree to which human error potential is incorporated or ignored. Even when assurance steps are embedded in the process analysis, this does not imply that human error is necessarily addressed.

Human Error

Similar to design and process risk, the human error domain is also replete with excellent methods and tools (Table 1). However, as human factors researchers and practitioners know, even validated methods and tools are only as valuable as the implementation is successful. Due to the inherent sensitivity of human errors, data collection and analysis can be easily undermined by numerous factors: high-level corporate philosophies and policies, as well as low-level group norms and lack of trust. Many specific tools including MEDA^{d,e} and HFACS-ME^f, and generic tools such as root cause analysis, cognitive task analysis and the assessment of performance shaping factors provide methodological options for identifying, organizing, describing and measuring human error behaviors. Systems of contributing factors or performance shaping factors can be extensively delineated, as well as links to intervention strategies. Limitations with respect to the hardware and process contexts in which errors occur vary in relevance depending

on the type of questions asked. In many cases, management decisions cross the risk type boundaries. For instance, do workmanship errors that cause hardware damage suggest training interventions or do they suggest a change in hardware vendors? Do procedural violations suggest amended procedures, policy changes, personnel actions, or a consideration of all three? Strictly human error descriptions provide information on their own, but in many cases they will point to the need for further evaluations of the hardware and process contexts.

Table 1. Examples of Different Types of Risk Assessment

Risk Type	Target	EXAMPLE
DESIGN RISK	Engineering Object <ul style="list-style-type: none"> • Vehicle Systems • Subsystems, Components 	<p>Space Shuttle PRA that quantifies risk drivers of the vehicle aids some design decisions on how to reduce risk most effectively in the Shuttle Upgrades Program^g</p> <p>LIMITATION: Cannot specify inspection controls at the procedural level; cannot predict or explain human error in maintenance and inspection</p>
PROCESS RISK	Operational Process <ul style="list-style-type: none"> • Requirements • Procedures, Tests • Maintenance 	<p>Boeing procedure and process analysis of 737 CFM56 Engine Change aids improvements to procedures, GSE recommendations, and hardware changes^h</p> <p>LIMITATION: Incorporated HF informally but not systematically analyzed; incorporated some hardware comparisons, but not at a design risk level</p>
HUMAN ERROR	Human Performance <ul style="list-style-type: none"> • Accidents • Incidents • Wear and Tear • Collateral Damage 	<p>Investigation of wire arcing on shuttle launch found to be the result of collateral damage. Human error potential points to ground processing factors such as standardized visual inspection, maintenance workplace and practicesⁱ</p> <p>LIMITATION: Cannot address issues of wire aging characteristics, adequacy of electrical integrity checks, effects of excessive modifications and repairs</p>

Risk Assessment Mismatches

Given the quantity and variety of risk assessment methods, there seems to be no lack of tools to answer a wide range of risk management questions. At least on an independent basis, design, process and human error risk can be targeted and evaluated. The danger lies in using one type of assessment to address issues that are outside its targeted domain. Two examples follow that point out potential mismatches.

Using Design Risk Analysis to Address Human Error

Currently, shuttle PRA models utilize a sophisticated combination of both qualitative (FMEA/CIL) and quantitative risk assessments. While suitably relevant to design issues, they fail to account for process reliability or human errors associated with maintenance and inspection. In

contrast, most operational issues and changes discussed in the recent Space Shuttle Independent Assessment Reportⁱ (e.g., reduction of inspection points, deferral of maintenance, organizational changes, increased technician responsibilities, extended overtime, increase in low-time technicians) do require process and human error risk considerations. In omitting human error estimates, it is equivalent to assuming (or demanding) perfect, error-free maintenance and inspection. In spite of the fact that in shuttle ground process, there are numerous tools and initiatives for acquiring information related to mishaps, human error events and workmanship problems, data representing human error estimates have not been incorporated into existing shuttle PRA models

Using Human Error Metrics to Address Process Risk

Significant industry attention has been drawn to human error data collection and management, and the maintenance community (in ATA Specification 113) considers this activity to be an important element in Safety and Human Factors program^j. While it is acknowledged that data collection and management are not trivial to achieve, a system that is successfully implemented will contain useful data; data that can provide guidance for process improvements, training interventions, policy-level changes, etc. However, thorny issues associated with both quantity and quality of data can reduce the usefulness of human error analysis. For example, quantity of data is a perennial problem since the size of accident and incident databases often limits its generalizability. As “tip of the iceberg” events, it is difficult to assess their significance when the size and shape of the iceberg below is unknown. When we move lower in the event database, to events of greater quantity such as problem reports, quality of information often becomes an issue. Once events are described at the task level, they are seldom accompanied by human error characterization because it becomes a massive undertaking to perform human error assessment on that scale (i.e., characterizing all workmanship errors at a level of detail comparable to that of incident and accident data).

Integrated Approaches to Assessing Risk

Table 1 illustrated how different types of risk assessments can aid decisions in which the risk types and targets are consistent on a one-to-one basis; when design risk assessment aids design decisions, process risk assessment aids process decisions, and so forth. In the examples above, instances are described where risk assessments have been applied beyond their limitations. Now, I would like to provide two examples in which risk assessment techniques have been combined in order to consider more than one risk type and to broaden their combined relevance to risk management questions.

Human Error Analysis in the Context of Process Risk

A three year project (1995-97) was sponsored by NASA, and conducted by the Idaho National Engineering and Environmental Laboratory (INEEL) in collaboration with Boeing with airline support^k. The project focused on a process level analysis called Human Error Analysis (HEA) applied to aviation maintenance tasks in order to develop a framework for maintenance

activities. In part, the project investigated the human error level by elaborating potential error types (4 types of omission errors and 41 types of commission errors) for airplane maintenance. It then elaborated general, intermediate and specific levels of performance shaping factors (or contributing factors). At this point, the tool (called Framework Assessing Notorious Contributing Influences for Error, or FRANCIE) falls in the category of other human error analysis tools, such as MEDA (which was deliberately incorporated). However, using FRANCIE in the context of a task analysis, the elaboration of any given error type was quantified through the assignment of human error probability values (determined through expert estimates). These estimates consisted of ratings of performance shaping factors for each error type. Once probability values were estimated, they were used to calculate failure paths and to identify dominant error chains.

In developing a set of methods and tools adapted to the maintenance tasks, a case study was made of the “Installation of the Master Chip Detector (MCD)” task for three airplane designs. Human errors resulting in an oil leak past the MCD or through MCD housing, given it was not replaced properly, were the focus of the HEA/HRA modeling effort. Maintenance procedures were modeled using an HRA event tree approach (THERP)¹ that showed how maintenance tasks were related and the consequences of failures and recoveries on individual subtasks. Although actual maintenance error rates were not available, estimates from other industry data were close enough to generate overall error rates that were consistent with data obtained from operational experience. The successful modeling and development of prototype software tools limited its investigation to only one type of maintenance error, but the importance of this study was its proof of “approach” and its innovative combination of existing risk assessment tools across process and human error boundaries.

Process Reliability in the Context of Design Risk

A current project focusing on process reliability in visual inspection provides another integrated approach to risk assessment. This NASA supported project is conducted by Lee Ostrom at the University of Idaho and, again, involves both airline and Boeing collaboration. The project investigates whether the inspection process for crack detection can be improved by developing tools for determining optimum inspection points and intervals. Currently, inspection points and intervals are specified by the maintenance program which is based on manufacturer recommendations and regulatory approval.

Company inspection records provide detailed inspection data on crack detection. These records drive maintenance actions and conform to inspection requirements, but in of themselves, do not provide a metric of inspection reliability. Thus the information does not point to company-specific strengths and needs that can guide inspection program enhancements. A reactive approach might consist of a review of incident data for guidance even though the relevant data might be meager. In contrast, a proactive approach would seek guidance from actual inspector reliability metrics.

By going back to the manufacturer design analyses (fatigue crack analyses and damage tolerance ratings), risk-based estimates of crack growth curves, combined with estimates of human reliability determine inspection requirements. Through reverse engineering, actual inspection data can be used in combination with the crack growth propagation curves to generate more accurate inspection reliability estimates, which then can be compared to the original industry estimates. Since company data can be broken down in many ways (e.g., aircraft, zones, inspection type, facilities, shift, vendor, if outsourced) different reliability metrics can be

compared within company, and on this basis, specific inspection program questions can be asked and improvement decisions can be aided. This project is still ongoing but the results are promising and we hope the research can provide a model and set of methods for determining ones own visual inspection reliability.

Summary

Risk assessment has been growing as a discipline, offering a proliferation of tools and methods, as well as a growing research base in which applications are being validated in more domains. In addition, risk assessment, known more for its use in design applications, has been expanding its reach to processes and human error. With these extensions, there has been some confusion of risk types resulting in assessments of one risk type addressing issues beyond its targeted domain. In some cases, these can be dangerous mistakes, so we are pressed to find better solutions for answering complex risk management questions. Because many operational decisions simultaneously address interdependent design, process and human error risks, integrated approaches may be needed.

Two approaches were described that cross the boundaries of design, process and human error; the first providing a test case and tools for analyzing human error and performance shaping factors within the aircraft maintenance domain. The approach goes beyond error analysis to generate probabilistic estimates of error within a task/procedural context through fault tree analysis. The second approach integrates inspection detection records (process level data) in the context of design risk estimates in order to generate actual inspection reliability metrics. Both approaches have integrated different types of risk information through innovative combinations of analysis tools. Risk management decisions that are narrower in scope may continue to be satisfied with single approach solutions, but resolving complex operational issues within an environment with constrained resources may be better served by more flexible and integrated approaches.

REFERENCES

- a. Fragola, J., et al. (1995) *Probabilistic Risk Assessment of the Space Shuttle*, NASA/HQ Code M. Washington DC 20546, 28 February 1995, CASI Record No. 95N26398.
- b. Kumamtot, H., and Henley, E., *Probabilistic Risk Assessment and Management for Engineers and Scientists*, IEEE Press, 1996.
- c. Fragola, J. (1996). Space Shuttle Probabilistic Risk Assessment in *1996 Proceedings Annual Reliability and Maintainability Symposium*.
- d. Allen, J. P., Jr., & Rankin, W. L. (1996). Use of the Maintenance Error Decision Aid (MEDA) to enhance safety and reliability and reduce costs in the commercial aviation industry. In *Meeting Proceedings Tenth Federal Aviation Administration Meeting on Human Factors Issues in Aircraft Maintenance and Inspection Maintenance performance enhancement and technician resource management* (pp. 79-87). Washington, DC: Federal Aviation Administration/Office of Aviation Medicine.
- e. Rankin W.L. and Allen, J.P., Jr. (1996). Boeing introduces MEDA: Maintenance Error Decision Aid. *Airliner*, April-June, 20-27.
- f. Schmidt, J., Schmorow, D. D., & Hardee, M. (1998). A Preliminary Human Factors Analysis of Naval Aviation Maintenance Related Mishaps. *SAE AEMR Conference Proceedings*, Long Beach, CA.
- g. *Upgrading the Space Shuttle Report* (1999). National Research Council Committee on Space Shuttle Upgrades, Washington, DC, National Academy Press.
- h. Repp, T. (1995, October-December). Improving 737 CFM56 engine change times. *Airliner*. Seattle, WA.
- i. *Shuttle Independent Assessment Team Report* (2000). National Aviation and Space Administration, Office of Space Flight. http://www.hq.nasa.gov/osf/shuttle_assess.html
- j. Air Transportation Association (ATA) Specification 113: *Maintenance Human Factors Program Guidelines*. <http://www.airlines.org/public/publications/display1.asp?nid=938>
- k. Ostrom, L. Nelson, W., Haney, L. N., Richards, R. Wilhelmsen, C., Owen, R. (1997) *Structured Human Error Analysis for Airplane Maintenance and Design*. Idaho National Engineering Laboratory, Lockheed Martin Idaho Technologies Company, Report INEEL/EXT-97-01093, October, 1997.
- l. Swain, A. D., and Guttman, H. E. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, SAND80-0200.